# 線形符号の最大符号長について (情報理論・実験計画法における組合せ数学の諸問題 II : 研究会報告集)

AUTHOR(S):

福田, 悌次郎

CITATION:

福田, 悌次郎. 線形符号の最大符号長について (情報理論・実験計画法における組合せ数学の諸問題 II : 研究会報告集). 数理解析研究所講究録 1970, 95: 56-66

ISSUE DATE:

1970-08

URL:

http://hdl.handle.net/2433/108168

数理解析研究所講究録
95巻 1970年 56-66



# 線形符号の最大符号長について

海上保安大　福田　悌次郎

## §1. 序

ガロア体 $GF(q=p^e)$ 上の $r\times n$ 行列 $H=\|h_{ij}\|$ $(i=1,2,\cdots,r;\ j=1,2,\cdots,n)$ が次の2つの性質を持つとき，$t$-independent であるという。

$$\begin{cases}(i) & \text{rank } H = r\\ (ii) & H\text{の任意の}t\text{列が1次独立である。}\\ & \text{ただし，}\ 0<t\leqq r<n.\end{cases}\qquad(1.1)$$

$t$-independent な行列をパリティーチエック行列に持つ $GF(q)$ 上の線形符号は最短距離 $d=t+1$ の $(n,\ k=n-r)$ code であるが，$t$ と $r$ を固定したとき上記の条件(i),(ii)を充す $n$ の最大値 $m_t(r,q)$ を求めるという問題は一般に未解決である。

この問題は単に最も効率のよい符号を求めるという誤り訂正符号理論だけでなく，情報検索におけるファイル構成や実験計画法，特に要因計画における一部実施法とも密接に関係している。

本稿では $m_t(r,q)$ に関してこれまでに得られた部分的結果について報告する。

## §2. $m_t(r,q)$ の値について

1942年 R. A. Fisher が始めてこの問題を実験計画法の立場から取上げ，$t=2$ の場合に次の結果を得た。

$$m_2(r,q)=\frac{q^r-1}{q-1} \qquad (2.1)$$

次いで1947年，R. C. Bose [1] は $m_t(r,q)$ が $GF(q)$ 上の $(r-1)$ 次元射影空間におけるどの $t$ 個の点も1次独立であるような点集合の濃度の最大値を表わすということに着目して次の結果を示した。

$$\begin{cases} m_3(3,q)=\begin{cases} q+2 & (q=2^l \text{のとき}) \\ q+1 & (q=p^l,\ p\neq 2 \text{のとき}) \end{cases} \\ m_3(4,q)=q^2+1 \qquad (q=p^l,\ p\neq 2 \text{のとき}) \\ m_3(r,2)=2^{r-1} \end{cases} \qquad (2.2)$$

更に，$t=2u$ のとき $n=m_t(r,q)$ とおくと $n$ は

$$q^r \geqq 1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\cdots+\binom{n}{u}(q-1)^u \qquad (2.3)$$

という不等式を充さねばならないことを示した。

この不等式は符号理論では Hamming bound と呼ばれているものである。

以下基礎体を $GF(2)$ に限定して論ずることにする。

## 1. $t=3$ の場合

この場合は(2.2)式 $m_3(r,2)=2^{r-1}$ により完全に解決している。これは $n=2^{r-1}$, $k=2^{r-1}-r$, $d=4$ を parameters とする code で，修正 Hamming code と呼ばれており，GF(2) 上の $(r-1)$ 次元射影空間 $PG(r-1,2)$ における一つの超平面の補集合をパリティー行列に選ぶことによって得られる[1],[6]。

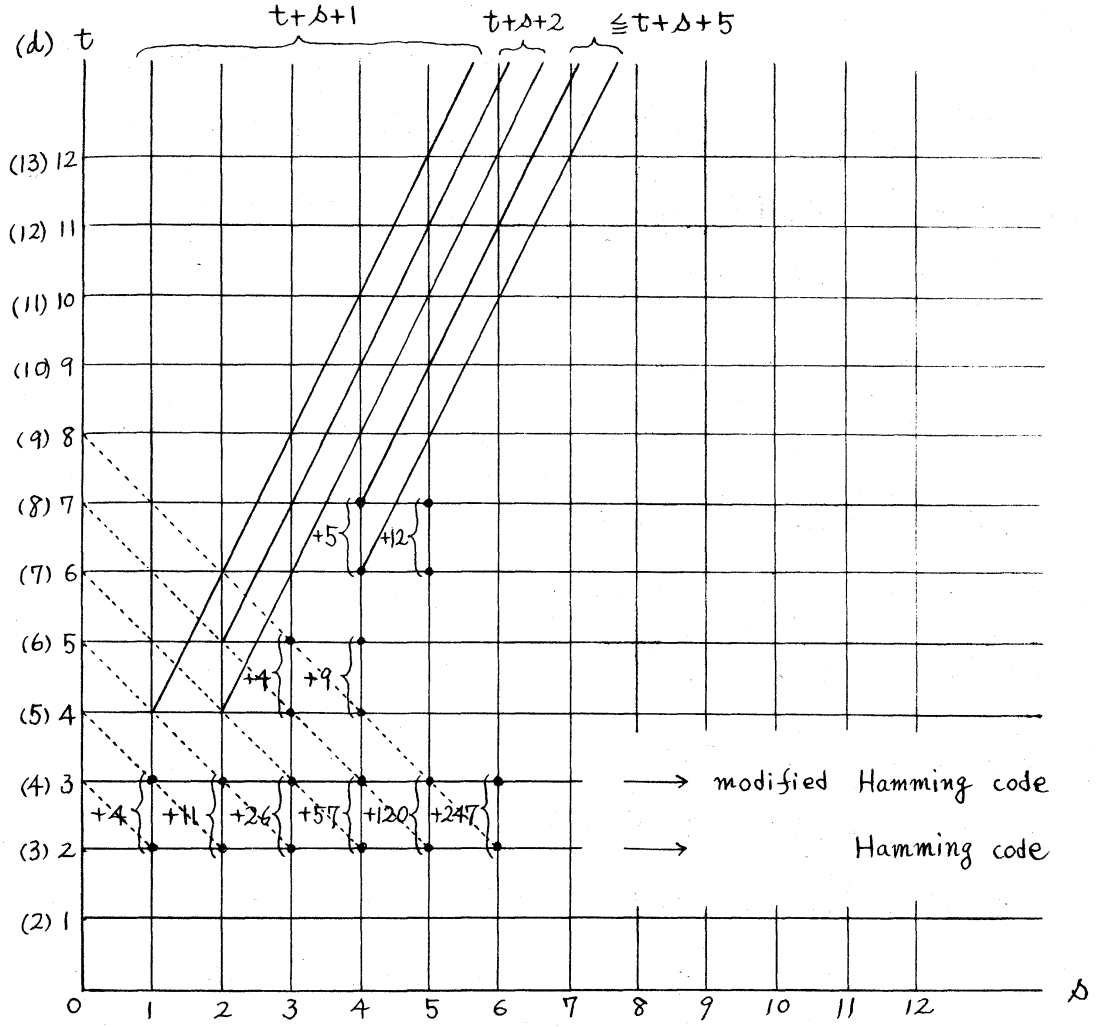
## 2. $t\geqq 4$ の場合

1969年 B.R. Gulati[3] は $r$ を $r=t+s$ と分解して，次の結果を得た。

$$m_t(t+s,2)=\begin{cases} t+s+1 & (t\geqq 2s+2;\ s\geqq 1 \\ t+s+2 & (t=2s,2s+1;\ s\geqq 2) \\ \leqq t+s+5 & (t=2s-2,2s-1;\ s\geqq 4) \end{cases} \qquad (2.4)$$

これを図示すると次の通りである。

尚，$r=t+s$ の立場から統一的に眺めるため，Hamming code 並びに修正 Hamming code の符号長についても $t+s+k$ の形で表わしてグラフ上に記入しておく。




(註) +k は t+δ+k を表わす

上記 Gulati の結果に関連して，その周辺のいくつかの未知の部分について判ったことを次に列記してみる。

(1) δ=3 ; t=4, 5 の場合

δ=3 のときは次の不等式が知られている〔2〕.

$$t+\delta+1 \leqq m_t(t+\delta, 2) \leqq t+\delta+4 \qquad (2.5)$$

この場合は k=4 の Solomon-Stiffler code 並びに MacDonald

code によって upper bound を attain することが判る。即ち

$$\begin{cases} \Delta=3,\ t=4: & \text{Solomon-Stiffler} & n=11,\ k=4,\ d=5 \\ \Delta=3,\ t=5: & \text{MacDonald} & n=12,\ k=4,\ d=6 \end{cases} \quad \text{——(2.6)}$$

(2) $\Delta=4$; $t=6,7$ の場合

(2.4) の不等式から $m_t(t+\Delta, 2) \leqq t+\Delta+5$ であるが，この場合も $k=5$ の Solomon-Stiffler 並びに MacDonald code によって upper bound を attain する。即ち

$$\begin{cases} \Delta=4,\ t=6: & \text{Solomon-Stiffler} & n=15,\ k=5,\ d=7 \\ \Delta=4,\ t=7: & \text{MacDonald} & n=16,\ k=5,\ d=8 \end{cases} \quad \text{——(2.7)}$$

(3) $\Delta=4$; $t=4,5$ の場合

$\Delta=4$ のときは次の不等式が成立する[2]。

$$t+\Delta+1 \leqq m_t(t+\Delta, 2) \leqq t+\Delta+9 \quad \text{——(2.8)}$$

ところで $t=4$ のときは，(2.8) の upper bound を attain する code が存在することを Prange が示した[4]。即ち

$\Delta=4,\ t=4$: Prange $n=17,\ k=9,\ d=5$ ——(2.9)

したがって，$B(n, 2u+1) = B(n+1, 2u+2)$ の関係から

$\Delta=4,\ t=5$: $n=18,\ k=9,\ d=6$ ——(2.9)′

という parameters を持つ code も存在して，maximal である。

(4) $\Delta=5$; $t=6,7$ の場合

$n=23,\ k=12,\ d=7$ を parameters とする Golay code は perfect code であることが知られている。即ち

$r=t+\Delta=6+5=11$, $t=6$ という条件の下で Hammingの不等式 $2^{11} \geqq \sum_{i=0}^{3}\binom{n}{i}$ を充す最大の整数は $n=23$ (実は upper bound を attain している) という意味で maximal code である。

よって

$\Delta=5, t=6$ : Golay　　$n=23, k=12, d=7$ ——— (2.10)

また, $B(n, 2u+1)=B(n+1, 2u+2)$ の関係から 次の parameters を持つ code も maximal である。

$\Delta=5, t=7$ :　　$n=24, k=12, d=8$ ——— (2.10′)

(5) $\Delta=0$ の場合は, すべての $t$ の値に対して $m_t(t+\Delta, 2)=t+\Delta+1$ であることは明らかである。

(2.4)式並びに以上(1)～(5)の結果から, $m_t(r, 2)$ の値は $r \leqq 8$ の場合にはすべて判ったことになる。

## 3. $t=4$ の場合

最近, E. Seiden [5] は, 射影空間 $PG(r-1, 2)$ においてどの4点も共面ではないような点の集合はどのような構造を持っているかという観点から $m_4(r, 2)$ の研究を行った。

主要結果は次の通りである。

$$\begin{cases} m_4(4,2)=5 \\ m_4(5,2)=6 \\ m_4(6,2)=8 \end{cases} \qquad \text{(2.11)}$$

$$m_4(7,2) = 11 \qquad (2.11)$$

$$m_4(r,2) \leqq 3(2^{r-6}-1)+8 \quad \text{for} \quad r \geqq 8 \qquad (2.12)$$

特に，$r=8$ のときは等号が成立する．　即ち

$$m_4(8,2) = 17 \qquad (2.13)$$

これらの結果は (2.6) 式の Solomon-Stiffler code や (2.9) 式の Prange code の maximality を列の角度から保証している。

因みに，(2.13) の解は次の通りである。

$$H = \left[\begin{array}{ccccccccc:c} 1&1&0&1&1&0&1&0&0 & \\ 1&1&0&1&0&1&0&0&1 & \\ 1&1&0&0&1&1&0&1&0 & \\ 1&1&1&0&0&1&1&0&0 & I_8 \\ 1&1&1&0&1&0&1&1&1 & \\ 1&0&1&1&0&1&0&1&0 & \\ 1&0&1&1&1&1&1&0&1 & \\ 0&1&1&1&1&1&0&1&1 & \end{array}\right] \qquad (2.14)$$

尚，Seiden による upper bound (2.12) と $2^r \geqq 1+\binom{n}{1}+\binom{n}{2}$ を充す $n$ の最大値，即ち，Hamming bound を比較すると $r=8$，$r=9$ の場合は (2.12) の方が良いが，$r \geqq 10$ となると逆になる。

| | Seiden bound | Hamming bound |
|---|---|---|
| $r=8$ | 17 | 22 |
| $r=9$ | 29 | 31 |
| $r=10$ | 53 | 44 |

## 4. Seiden bound の一般化

$t=4$ の場合の Seiden の不等式(2.12)は，次のようにして一般化することが出来る。

これに先だって，$GF(q)$ 上の有限次元射影空間におけるよく知られた Lemma を用意する。

[Lemma]

$g, e$ を $0 \leqq e < g < r-1$ を充す任意の非負整数とすると，

$PG(r-1, q)$ において一つの $e$-flat を含む $g$-flats の個数は

$$\Phi(r-e-2,\ g-e-1,\ q) \qquad (2.15)$$

で与えられる。

(註) $\Phi(f, g, q)$ は $PG(f, q)$ における $g$-flats の個数を表わす記号で，その値は次式で与えられる。

$$\Phi(f, g, q) = \frac{(q^{f+1}-1)(q^{f}-1)\cdots(q^{f-g+1}-1)}{(q^{g+1}-1)(q^{g}-1)\cdots(q-1)} \qquad (2.16)$$

この Lemma を使うと次の定理が成り立つ。

[定理]

$$m_t(r, 2) \leqq 3\, m_t(r-1, 2) - 2\, m_t(r-2, 2) \qquad (2.17)$$

(証) $PG(r-1, 2)$ において，一つの $(r-3)$-flat $V$ を考えると $V$ に含まれている $t$-independent な点の個数の最大値は $m_t(r-2, 2)$ である。この $t$-independent な点の集合を $S$ としよう。

次に，$V$ を含む $(r-2)$-flats の個数は上の Lemma により

$$\phi(r-(r-3)-2,\ (r-2)-(r-3)-1,\ 2)$$
$$=\phi(1,0,2)=\frac{2^{1+1}-1}{2-1}=3$$

即ち，$PG(r-1,2)$ において $V$ を含む 3 つの超平面 $V_1, V_2, V_3$ が存在する。

$V_i$ $(i=1,2,3)$ は $(r-2)$ 次元であるから $m_t(r-1,2)$ 個の $t$-independent な点から成る部分集合 $T_i$ を含み，かつ，$S \subset T_i$ ならしめ得る。

よって，次の不等式を得る。

$$m_t(r,2) \leqq 3\left[m_t(r-1,2)-m_t(r-2,2)\right]+m_t(r-2,2)$$
$$=3m_t(r-1,2)-2m_t(r-2,2)$$

Q.E.D.

(註) Seiden bound は $t=4$, $r=8$ の場合に相当する。

尚，この定理を使うと (2.4)式の Gulati bound に対する次のような別証明が得られる。

(i) $t=2s-1$, $s \geqq 4$ の場合

(2.4) の最初の 2 つの等式を使うと

$r-1=t+(s-1)$ に対しては $t=2(s-1)+1$ であるから

$$m_t(r-1,2)=t+(s-1)+2=2(s-1)+1+(s-1)+2=3s$$

$r-2=t+(s-2)$ に対しては $t=2(s-2)+3$ であるから

$$m_t(r-2,2)=t+(s-2)+1=2(s-2)+3+(s-2)+1=3s-2$$

$\therefore \quad m_t(r,2) = m_t(t+\Delta, 2) \leqq 3\cdot 3\Delta - 2(3\Delta-2)$

$= 3\Delta + 4 = (2\Delta-1) + \Delta + 5$

$= t + \Delta + 5$.

(ii) $t = 2\Delta-2$, $\Delta \geqq 4$ の場合も (i) と同様にして

$r-1 = t+(\Delta-1)$ に対しては $t = 2(\Delta-1)$ であるから

$m_t(r-1, 2) = t+(\Delta-1)+2 = 2(\Delta-1)+(\Delta-1)+2 = 3\Delta-1$

$r-2 = t+(\Delta-2)$ に対しては $t = 2(\Delta-2)+2$ であるから

$m_t(r-2, 2) = t+(\Delta-2)+1 = 2(\Delta-2)+2+(\Delta-2)+1 = 3\Delta-3$

$\therefore \quad m_t(r,2) = m_t(t+\Delta, 2) \leqq 3(3\Delta-1) - 2(3\Delta-3)$

$= 3\Delta + 3 = (2\Delta-2) + \Delta + 5$

$= t + \Delta + 5$.

# 参考文献


[1] Bose, R. C.(1947): Mathematical theory of the symmetrical factorial designs. Sankhyā vol.8, 101—166.

[2] Gulati, B. R.(1969): Some useful bounds in symmetrical factorial designs(Abstract). A.M.S., vol. 40, 723.

[3] Gulati, B. R.(1969): Useful bounds in symmetrical factorial designs and error correcting codes (Abstract). A.M.S., vol. 40, 1514.

[4] Peterson, W. W.(1961): Error correcting codes. MIT Press and Wiley, New York.

[5] Seiden, E.(1969): On the problem of construction and uniqueness of saturated $2_R^{K-p}$ designs. Inst. Statis. mimeo. series 600.19, Chapel Hill, N.C.

[6] 福田悌次郎(1970): Algebraic coding theory における二,三の話題. 京大数解研講究録 82, 1—11.